

Formal security analysis of registration protocols for interactive systems: a methodology and a case of study

Jesus Diaz, David Arroyo, Francisco B. Rodriguez

September 7, 2012

Abstract

In this work we present and formally analyze CHAT-SRP (**CHA**os based **T**ickets-**S**ecure **R**egistration **P**rotocol), a protocol to provide interactive and collaborative platforms with a cryptographically robust solution to classical security issues. Namely, we focus on the secrecy and authenticity properties while keeping a high usability. In this sense, users are forced to blindly trust the system administrators and developers. Moreover, as far as we know, the use of formal methodologies for the verification of security properties of communication protocols isn't yet a common practice. We propose here a methodology to fill this gap, i.e., to analyse both the security of the proposed protocol and the pertinence of the underlying premises. In this concern, we propose the definition and formal evaluation of a protocol for the distribution of digital identities. Once distributed, these identities can be used to verify integrity and source of information. We base our security analysis on tools for automatic verification of security protocols widely accepted by the scientific community, and on the principles they are based upon. In addition, it is assumed perfect cryptographic primitives in order to focus the analysis on the exchange of protocol messages. The main property of our protocol is the incorporation of *tickets*, created using digests of chaos based *nonces* (numbers used only once) and users' personal data. Combined with a multichannel authentication scheme with some previous knowledge, these tickets provide security during the whole protocol by univocally linking each registering user with a single request. This way, we prevent impersonation and Man In The Middle attacks, which are the main security problems in registration protocols for interactive platforms. As a proof of concept, we also present the results obtained after testing this protocol with real users, at our university, in order to measure the usability of the registration system.

1 Introduction

Modularity is one of the most relevant aspect of modern engineering practices. Regarding cryptographic applications, this property resorts to distinguishing the

formal aspect of cryptographic protocols from the inner details of the underlying algorithms (see [2, 24]). In this vein, we can design strong cryptographic algorithms for confidentiality, integrity and authentication, but applying them incorrectly would lead to security flaws. Therefore, the study of the security of a cryptographic protocol demands to examine the security of cryptographic primitives from a computational point of view, but also to evaluate the goodness of the integration of those primitives. In this work we propose a registration protocol for interactive platforms.

The proper design and evaluation of cryptographic protocols is critical when personal information is exchanged. This is the case of interactive and collaborative platforms, which are of great importance in the current state of communications, specially after the irruption of web 2.0 technologies. This type of applications are used to share and exchange information, even critical personal data [35]. Nonetheless, users' trust is generally implicitly assumed and there is no explicit application of procedures to secure users' registration and exchange of information. In the context of interactive applications, and always from a general point of view, the main properties of the underlying security system rely completely on the correct implementation and subsequent management of the system. Privacy, secrecy and authenticity are assumed when users get into the system, i.e., by adhering straightway to solutions provided by administrators and developers. In this sense, the only way to incorporate the basics of information security is through properly using standard tools proposed, evaluated and validated by the cryptography and information security community.

On the regard of applying standard and validated technologies, we have previously introduced a registration protocol to enhance interactive platforms' security [17]. This registration protocol links each user to a digital identity, giving users access to the cryptographic tools sustaining confidentiality and authenticity, i.e., (client-side) encryption and digital signatures. The service provided by our registration protocol could seem similar to the protection given by SSL-tunneled communications. Nevertheless, it rather complements SSL instead of overlapping its functionality: SSL provides secrecy and server side authentication, whilst client-side authentication cannot be provided by SSL as long as the client does not have a digital identity, which he would have once incorporated our protocol into the system. Moreover, thanks to the distribution of digital identities, and the cryptographic functionality they make available, their information may be also protected in the servers, since it can be encrypted or signed at client side. Therefore the sensitive information will be protected not only during the communications. And even more, this way, users will have a greater (and justified) sensation of security, which contributes to preserve a very important property (when it is correctly grounded) of information security systems: users' confidence in the system.

In this work we further refine the previous protocol, and formally analyse its security properties. Our protocol is based on **Email Based Identification and Authentication (EBIA)**, which links each new user to an email account. This kind of registration protocols for interactive platforms is widely extended in the internet. Nevertheless, there are two main security problems with these

protocols: impersonation and Man In The Middle (MITM) attacks. We tackle these problems here, proposing methods for circumventing them.

In any case, for guaranteeing that the ultimately distributed digital identities will successfully provide all their functionality, we need to ensure that we leave no unnoticed “security holes” in the registration protocol. To the best of our knowledge, and from a general point of view, implementation and design of registration protocols are not evaluated according to a formal methodology and using specialized tools intended for that end, like [6, 12]. In our work, we address this problem incorporating a phase-divided methodology, and using formal tools (in our case, ProVerif [12]) for the verification of the required security properties. It is worth to emphasize that we restrain ourselves to analyzing the security of the protocol itself, i.e., of the exchange of messages, while assuming a perfect cryptography model for all the cryptographic primitives used. Additionally, the final step of our work is on testing the usability of the protocol, in practice. In order to test it in a real scenario, we have incorporated the protocol in a Moodle platform. Moodle is probably the most extended e-learning platform worldwide nowadays [21]. It is also a perfect example of interactive and collaborative platform managing lots of sensitive data. But even more, EBIA is one of the most used authentication modules when working with Moodle. Therefore, it is a suitable context to test our protocol in.

The rest of the paper is organized as follows. In Section 2 we make an outline of the basic registration protocols for interactive platforms and expose their main security problems. In Section 3 we explain the methodology followed during our work. Afterwards, in Section 4 we introduce our new protocol, covering the first four steps of the procedure proposed in Section 3 and justifying the decisions that have led us to its final form. Section 5 is dedicated to the last step of our methodology, centered on the formal verification of the protocol. In Section 5 we also treat the usability properties of CHAT-SRP, showing the results obtained during tests performed with real users. At last, we conclude in Section 6, with an overview of our work and some discussions on future work.

2 A brief security analysis of interactive registration protocols

Our registration protocol takes as starting point the *EBIA* approach, reinforcing it with robust cryptographic functionality to guarantee secrecy and authenticity. *EBIA* is the most widely used registration and authentication system in interactive and collaborative systems (see [22]). The reason of taking it as starting point is its high expansion and usability, as every user of the internet is accustomed to its principles. Basically, for a given email address, e.g. *alice@email.dom*, *EBIA* says that if somebody can read an email sent to *alice@email.dom*, then she/he is the legitimate owner of that email account. As a result, *EBIA assigns* her/his virtual identity to that email address. During the registration process, the user has to access an activation link sent in an email in order to activate the account

(this process is schematized in Fig. 1).

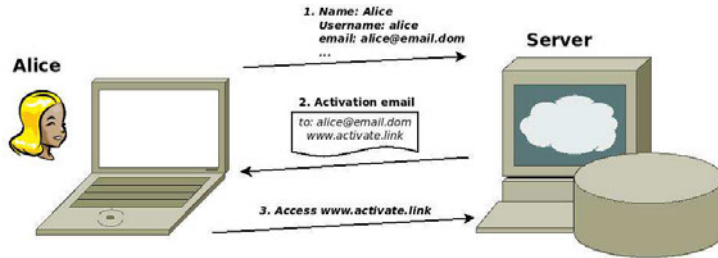


Figure 1: Behaviour of EBIA systems

(1) The user sends the request with his data. (2) The server validates the data and sends an activation link via email. (3) The user accesses the activation link.

Such a registration process presents two main security flaws. First, the activation email is sent unencrypted, which makes possible to mount a MITM attack (see [5, Chapter 2]). Let us consider the illustrative example shown in Fig. 2. If the attacker Eve wants to impersonate Alice in a web site using EBIA, she can proceed as follows: first, Eve waits until Alice sends a registration request to the Web Server (WS); then, the WS will send an activation email to Alice’s email account; after gaining control of an intermediary server, Eve intercepts the unencrypted email, gets the activation link, and blocks the email impeding to reach Alice’s email account; at last, Eve just needs to access the link in order to successfully complete the impersonation attack. As Alice did not receive an email, she will probably just think that an error occurred. As we discuss later, we use registration tickets for ensuring that whoever starts a registration request is the one obtaining the corresponding digital identity.

Now, let us assume that the previous problem is indeed solved. Then, the second problem is that if the attacker knows all the required data for a user to be registered, he can successfully impersonate him from the beginning. To the best of our knowledge, the easiest (and maybe only) solution to this problem is to link identities distribution with some previous information known by the registrar about the users. In this respect, and before the registration request, the registrar must possess some information concerning the user. This imposes very strong limitations to the contexts in which the resulting registration protocol will be suitable for. Nevertheless, there are many situations in which this is not an unreasonable requirement. In our case, we will require the registrar to know the mobile phone number of the users. With it, we will be able to perform a multichannel protocol with an authenticated channel (the mobile phone), which guarantees that the user completing registration is who claims to be.

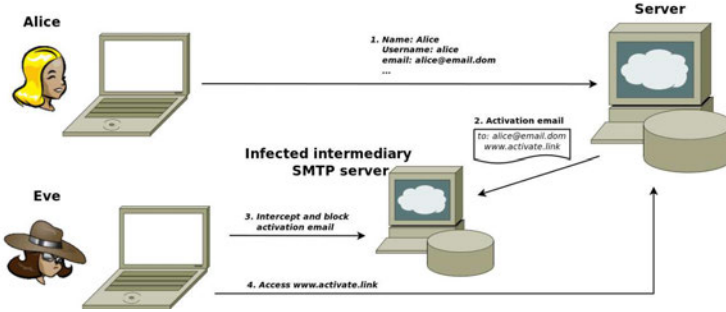


Figure 2: Attack to EBIA system. (1) Alice requests registration to the Web Server; (2) The server sends the activation email to Alice, containing the activation link, which passes through an infected intermediary server under Eve’s control. (3) Eve intercepts and blocks the activation email, and activates the account in Alice’s behalf. Alice will probably just think that an error occurred.

3 Methodology for design and verification of secure protocols

When considering implementation and design of registration protocols, the most common practice is adhering to a security model, design the protocol, and informally claim that the protocol is secure according to the assumed security model. In other words, security is assumed instead of being formally tested. The lack of a formal methodology to evaluate security leads to unnoticed errors, which may later cause severe damage to the protocols or even make them useless. Consequently, it is highly convenient to adopt methodologies based on the formal analysis of protocols, as the one applied in [36] for verification of an electronic voting system. In this vein, we propose the procedure schematized in Fig. 3, which consists of five stages. The first stage define the goals of our protocol, enabling the identification of critical aspects and the complexity of the associated problem. After this initial analysis, we have enough information to concrete an abstract model in coherence with the practical scenario where the protocol will run (second stage of the methodology). According to the security abstract model, in the third stage we formally define the security properties and discuss their feasibility. Sometimes, this “preliminary” analysis is omitted because we think that we perfectly know our context, and it is not worth the effort. However, as it is said in [26], it is desirable and beneficial to follow a methodological approach for establishing the desired security goals and requirements. Finally, the protocol is designed and formalized in order to be analyzed with automatic and proved tools (stages four and five).

It can be seen that the steps of our methodology follow a natural order. As far as we know, steps one and, sometimes, three are usually ignored, which can involve contradictions and/or disregarding of the relevance of some property.

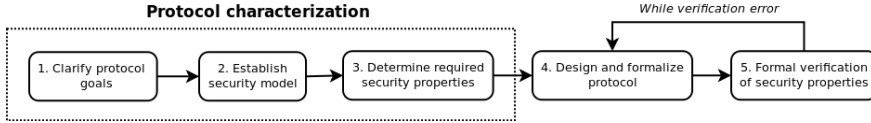


Figure 3: Proposed procedure for the creation and design of secure protocols: (1) Make clear the protocol goals; (2) Establish the security model and assumptions; (3) Determine the required security properties for achieving the goals; (4) Design and formalize the protocol; (5) Carry out a formal verification of the required security properties.

The second step, although it may be commonly applied in any explicit way, helps modelling the scenario and determining the security properties. These three first steps can be summarized in a more general phase: the protocol (and environment) characterization. Nevertheless it is worth separating them, since although related, they are intended for different aims. The fourth step could be introduced within the fifth one (since formal verification of the protocol demands its previous formalization), but it is worth to be considered separately, since improves the designer’s knowledge of the protocol. Note that we have included a loop back from the fifth to the fourth step, in case some security property is not held (we assume that if a security property is not possible in a given environment, it will be detected in the first three steps).

As we will see in the subsequent sections, we have followed this methodology for the design and evaluation of our protocol.

4 The proposed protocol: CHAT-SRP

In this section we present CHAT-SRP, our proposed registration protocol. We introduce here the first four steps of the proposed methodology, reasoning about why the main modifications over EBIA are necessary. We leave the formal security analysis for the following sections, where we will show that the impersonation and MITM attacks explained before are avoided.

4.1 Protocol characterization: goals, security model and security requirements

CHAT-SRP is a registration protocol mainly intended for interactive and collaborative platforms. Therefore, its goal is to provide new users with digital identities. These digital identities are intended to be used for cryptographic purposes, like encryption and digital signatures. Obviously, the user will take active part in the protocol. Also, several servers will interact between them during registration.

Regarding the assumed security model, we have based our analysis upon the Dolev-Yao model [18]. In it, the cryptographic primitives used are supposed to be perfectly secure, i.e., the attacker is not able to decipher the encrypted messages unless he has the corresponding decryption key, the random number generators create unpredictable random numbers, etc. Nevertheless, the attacker is assumed to be active, which means that he can intercept, resend, and insert messages. We take into account both external and internal attackers (see [15] for definitions concerning the *location* of the attacker). In order to model internal attackers, we allow the establishment of SSL sessions with the trusted third parties of the system. This way, an attacker has the capability to act from the inside.

A registration protocol is really an authentication protocol executed for a first time. As it is stated in [38], authentication protocols require two main properties: authentication and key distribution. The authentication property refers to being certain of the identity of the users, i.e., of the authenticity of *all* the data they provide, including their identities. The key distribution also deals with secrecy, assuring that the new users will be able to communicate with the rest of the principals preserving the confidentiality of the information transmitted through the network. Therefore, we will incorporate authenticity and secrecy into CHAT-SRP as a commitment.

4.2 Description of the protocol

Now we have covered the first three steps of the procedure (see Fig. 3). But before undertaking the fourth one, we explain in more depth the protocol internals. Once we have gained an in-depth knowledge of it, we will proceed with the formalization.

The principals involved in the protocol are four:

- The User, which is the one starting the protocol by asking for a new digital identity linked to her/his email.
- The Web Server (WS), which is the entity attending registration requests and acting as intermediary between the User and the Registration Authority. In addition, it generates the activation email, and performs some easy checks. *This is a trusted server!*
- The Registration Authority (RA), which is on charge of creating the tickets, i.e., of linking each user with a single ticket. *This is a trusted server!*
- The Certification Authority (CA), that creates the final digital identities upon requests of the RA. *This is a trusted server!*

The messages sequence between the principals is depicted in Fig. 4, where the continuous lines represent SSL protected communications (with server authentication), and the dashed ones represent unprotected communications. The unprotected communications are the messages 6.2 (email sent via SMTP) and the user accesses to the activation link through message 7.1. This last message

is modelled as unprotected because the communications are assumed not to be anonymized, and thus the attacker will be able to link the accessed URL and the user by listening on the communication channel. It is worth mentioning that in the diagram shown in Fig. 4 the activation email and the ticket are sent to the user as separate messages (messages 6.1 and 6.2 in the diagram). In addition, the user accesses the activation link and sends the ticket separately (messages 7.1 and 7.2 in the diagram). Nevertheless, in the formalization, both messages 6.1 and 6.2, and messages 7.1 and 7.2, are merged into messages 6 and 7, with unencrypted and encrypted parts.

Concerning the principals distribution across the network architecture, obviously the user is an independent component by itself; but the network architecture of the three servers, i.e., WS, RA and CA is configurable. This means that they can be all in the same physical server, each one at a different server, or WS and RA in one machine and the CA in another. This is up to the system administrator. It is usually advised to keep the CA at a safe place, even without direct connection to the internet, using a “proxy” between it and the requesting users¹. Typically, this proxy is the RA, which does have access to the internet to receive registration requests. A sample network architecture with each server at a different machine is depicted in Figs. 5 and 6, including the messages sent between them during the protocol. Both images correspond to the two main parts of the protocol. In the first part, the user makes the registration request, obtaining a ticket linked to his email and personal data along with an activation link; in the second part, the user utilizes that ticket in order to obtain his final digital identity.

4.3 Robust multichannel authentication

In order to get registered into a typical interactive system, a user has to provide some personal data, which will be used during the digital identity creation. This data typically consists at least on a name and surname, email, and probably some other optional data (like postal address, phone numbers, or some national/organizational identification number). It is known that all this data is not too hard to obtain by combining internet searches with techniques such as social engineering ([5, Chapter 2]), or phishing [32]. If the attacker knows all the personal data of the person he wants to impersonate (and that person is not already in the system), then the attacker just needs to start the registration process and supply all the needed data.

The problem exposed in the preceeding paragraph is exactly that of discerning between *authentication of origin* and *entity authentication*, as described in [34, p. 8]. The first refers to the fact of being sure *where* a message come from (for example, the machine *alice.ii.uam.es*), while the second refers to *who* sent it (for example *Alice*). As settled in [34], this difference is often unclear, maybe because the consequences of one usually overlap with the consequences of the other. To be even clearer, let us make use of a pedagogical example: Alice can

¹See, for instance, the example given at <http://www.ejbca.org/architecture.html>

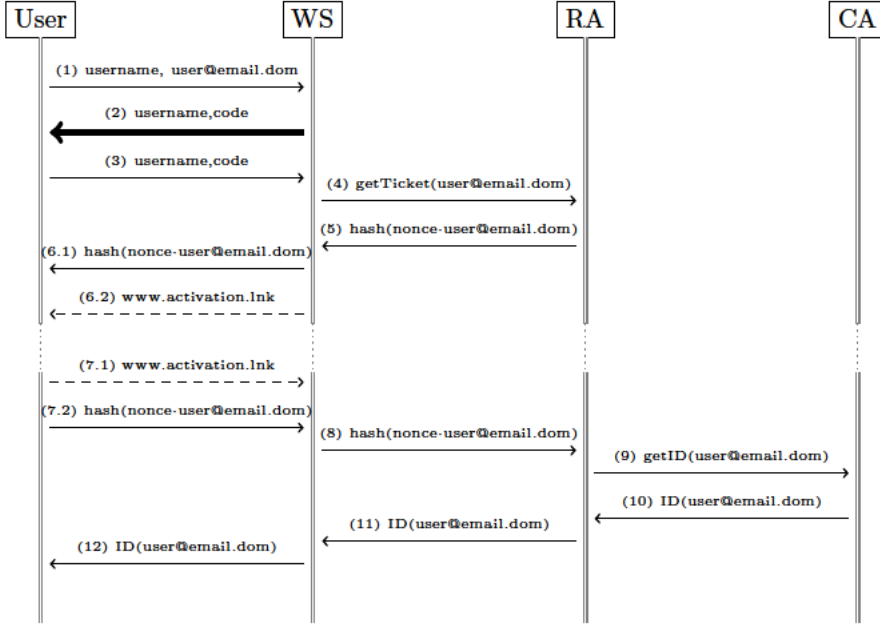


Figure 4: Sequence diagram of the messages exchanged during the protocol. The dashed lines represent unprotected communications; the thin continuous ones represent SSL protected communications, and the thick continuous line represents the message sent using the extra authenticated channel (SMS): (1) The user requests registration, providing his personal identification data; (2) The WS sends a code to the mobile phone number associated to the requesting user; (3) The user provides the received code to the WS; (4) The WS forwards the request to the RA; (5) The RA generates a ticket for the user, and sends it to the WS; (6.1) The WS forwards the ticket to the user via SSL; (6.2) The WS generates an activation link and sends it via SMTP to the user; (7.1) The user accesses the activation link; (7.2) The user sends the ticket to the WS; (8) After verifying the activation link, the WS forwards the ticket to the RA; (9) After verifying the ticket and deleting it, the RA requests the CA to issue a new digital identity; (10) The CA generates the user's digital identity and sends it to the RA; (11) The RA forwards the digital identity to the WS; (12) Finally, the WS forwards the digital identity to the user. Although it is not explicitly depicted, we assume that several different SSL sessions are established between the User and the WS during the registration process. Nevertheless, this will be modelled in the subsequent formalizations.

send a message from her host *alice.ii.uam.es*, which is legitimate. But if her host gets infected by *Eve*, then the communicating entity will be *Eve*, although the origin of the communication will still be *alice.ii.uam.es*. This is a clear violation

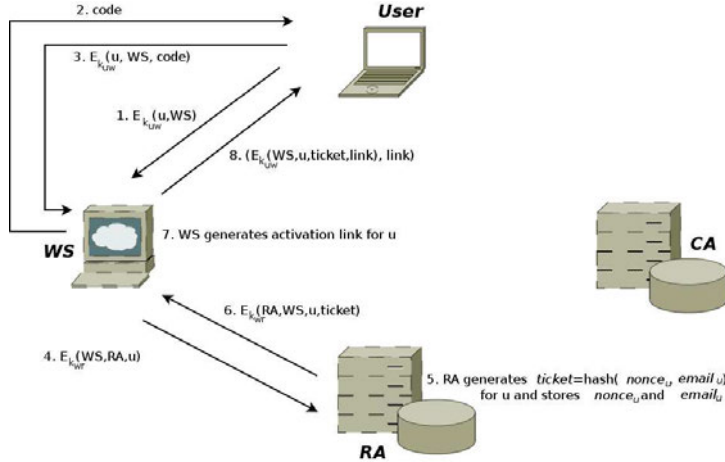


Figure 5: First half of the protocol: The user requests registration. After validating the user data, the WS sends an SMS with a code to the mobile phone number associated the new user. If the user correctly returns the code, the WS forwards the request to the RA, who generates a valid ticket linked to the user. When received the ticket, the WS also generates an activation link for that user, sending the ticket through SSL and the link via email. Here, k_{uw} represents the SSL key between the user and the WS, and k_{wr} represents the SSL key between the WS and the RA.

of the entity authentication property (see Fig. 7).

In [37] the authors propose the use of multiple channels, each with different security properties, in order to achieve authenticated communications. For example, they make use of an extra channel with low transmission capacity but which cannot be tampered with, although it may be subject to eavesdropping. This low capacity but secure channel is used to transmit a single bit of information, telling if the verification of the previous steps, carried on over a high capacity but unsecure channel, has been successful or not. If the outcome of such verification is positive, given their protocol, the communication will be *origin authenticated*. The authors in [19, 30] make a similar use of this multichannel combination in order to achieve *entity authentication*. Namely, they make use of mobile phones, which are used to receive and/or send a *One Time Pin* which will be returned in order to confirm they are the legitimate owners of that phone number. This is basically the same concept we used with emails, but with a subtle difference: users tend to control more tightly their mobile phones than their emails.

This subtle fact is something worth considering in some depth. In [19] it is reminded that there are basically three ways for verifying *entity authentication*: *KBA* or Knowledge Based Authentication (something you know), *TBA* or Token Based Authentication (something you have) and *BBA* or Biometrics Based

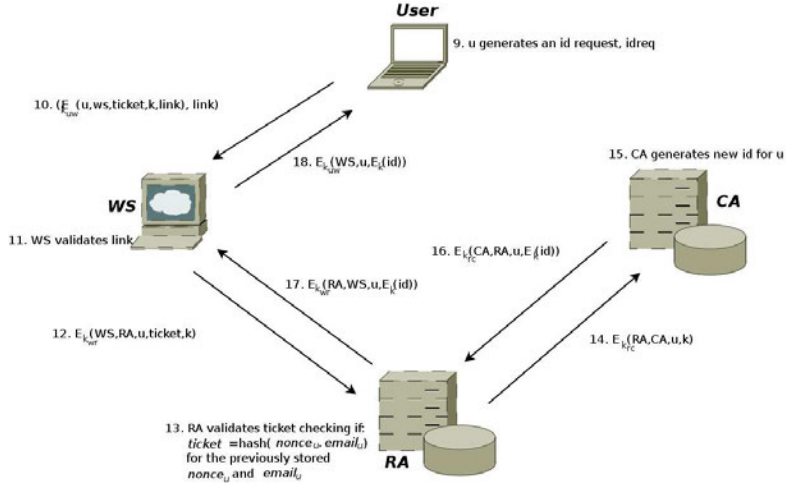


Figure 6: Second half of the protocol: The user generates a id request, accesses the activation link, and provides the registration ticket. After validating the user data, the WS forwards the ticket to the RA, who validates it using the nonce and email associated to that user, stored previously (see step 3 of Fig. 5), and requests the CA the generation of a digital identity for that user. The CA generates the ID and sends it to the user, passing through the RA and the WS. Here, k_{uw} represents the SSL key between the user and the WS, k_{wr} represents the SSL key between the WS and the RA, and k_{rc} represents the SSL key between the RA and the CA.

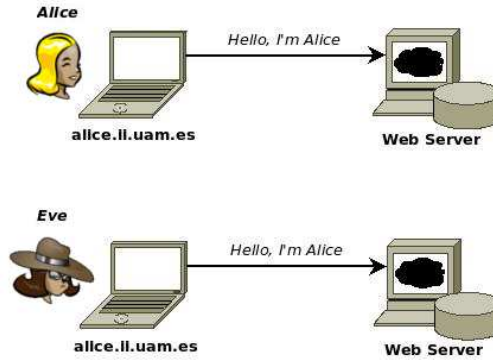


Figure 7: Illustration of identity theft violating entity authentication: If *Eve* gains control over Alice's host, the entity authentication property is broken.

Authentication (something you are). Nevertheless, there is a key concept that

is usually not even mentioned: the robustness of the authentication procedures is very dependant on the user perception about losing control of the supporting token or device, since a possible lost could be expensive or annoying. This fact is obvious for BBA (everyone tends to avoid losing his own fingers or eyes), but it is no that obvious for KBA or TBA. Even more for KBA, because people using TBA are usually more security-concerned users. And precisely, KBA is what affects us, because the problem we have is that we assume someone's identity based on personal data required and, maybe, the fact of knowing the password to access an email account.

So, as considered above, we need to provide our KBA system with something that makes the users think twice if their actions can lead to an annoying or undesirable situation, while keeping the usability of the system. The systems proposed in [19, 30] achieve precisely this property, providing a notorial improvement in security while not (or almost not) reducing usability. The use of mobile phones for this purpose suits our needs, as the fact of losing one's mobile phone leads to an annoying situation, since mobile phones are currently perceived as a more critical personal property than an email (maybe because they have physical presence). Therefore, the insertion of an additional step involving the sending of a message containing a One Time Pin or something similar could help us in our efforts to achieve *entity authentication*. Moreover, as observed in [37], it will also help the user to avoid attacks to his account. If a user receives a message at his mobile phone indicating that some action has been performed in her/his behalf, and he is not responsible for it, then someone must be trying to impersonate him, and he can just inform of the fact to thwart the attack. These reasons have led us to incorporate the extra mobile phone channel in order to overcome all the previously explained problems.

Nevertheless, there still exists a usability problem here. The perfect situation will be that in which the Service Provider (in our case, the WS) knows in advance the mobile number of the user. If not, then the attacker could simply provide the valid email of the user he wants to impersonate, and then give his own mobile number. This may be an unfeasible task for many of the web sites, but, for example, in the case of a university that wants its students and teachers to be registered in an e-learning platform, this is not such a hard measure. The university will simply need to ask their students/teachers to provide their mobile phone number when they get enrolled or hired. And from then on, the users will be able to use their mobile phones to authenticate themselves, and even to update their own mobile phone number.

4.4 Ticket generation

As it can be seen in the sequence diagram depicted in Fig. 4 and in Figs. 5 and 6, the ticket generation takes place at the RA after receiving its first message of the protocol. After validating the user data, and checking that no user with that email has already requested a ticket,² the RA creates a new one

²Other checks, like unicity of username, are done in the WS, but the RA only has to process the tickets.

for the requesting user. In order to do that, a nonce is generated. The nonce generation is of paramount importance to our protocol, as it is the element that allows us to assert that a user successfully retrieving a digital identity is the one who started the registration process. Therefore, we should adhere to the commitments of eSTREAM project³ to get an appropriate method to generate nonces. In our case, we have used a chaos based Pseudo-Random Number Generator [33]. Certainly, chaotic systems can be employed as skeleton of new, secure and efficient PRNGs (see [4]). Furthermore, cryptanalysis work in the field of chaos-based cryptography shows that security and efficiency can be achieved when there exists a proper combination of chaotic dynamics and the standards of conventional cryptography [3, 8, 7, 20].

Once obtained the nonce, it is concatenated with the user email, and passed through a one way hash function. This way, the user request has been univocally linked to the freshly created ticket. This ticket is sent securely to the user through messages 3 and 4, and it has to be returned later to the RA through messages 5 and 6 for the user to prove himself against the authority as the starter of the registration process. This very ticket is what prevents attacks like the one described in the Introduction, as only the user who started the communication is the one in possession of the correct ticket.

4.5 Comparison with EBIA

To be more clear about the reinforcements introduced by our protocol over EBIA, we summarize them here, restating the attacks avoided with their incorporation.

First, with the incorporation of the authenticated mobile phone channel we ensure that the users who succeed in the registration process are who they say they are. Note that the mobile numbers are previously known by the registrar (the WS in our case). In classic EBIA there is no way to avoid this, since there is no previous knowledge about the users. Even if the registrar knew that a specific email is indeed associated to a given user, since the email is inherently an insecure channel, it does not guarantee the authenticity (nor the secrecy) of the messages sent during the protocol.

Second, let us suppose that we want to use classic EBIA, but with the extra mobile phone authenticated channel. If, after the user successfully provides the code sent to him by the mobile phone, we carry on using classic EBIA, then the MITM attack depicted in Section 2 (Fig. 2) is still possible. Therefore, the previous multichannel authentication by itself does not guarantee anything if combined straightaway with classic EBIA. To reinforce this point, we have made use of tickets composed by nonces, which are used, among other purposes, to avoid replay and MITM attacks and provide *freshness* to the protocol messages [14]. The concept of tickets has been widely used in protocols and systems like Kerberos [31]. In our protocol, the user has to interact directly with the ticket created by the server. In fact, once tickets are generated, the user stores it in

³<http://www.ecrypt.eu.org/stream/>

her/his computer in order to prove her/his when demanded. In our protocol, tickets are generated by applying a one-way hash function (in our case, SHA-2) to the concatenation of a nonce [5, Chapter 3], and the identifier of the email account of the requesting user. Nonces are generated from a chaos based **P**seudo **R**andom **N**umber **G**enerator (PRNG) (see [33]), and the resulting ticket is sent through an SSL-protected channel when the user applies for registration. Therefore, each ticket is univocally linked to a single request, since it is used as a receipt when asking for a digital identity and subsequently discarded. This way only who initiates the registration request will be able to complete it, solving the problem of sniffing the activation link.

5 Security and usability analysis of the protocol

In the following sections we depict the secrecy and authenticity analysis by using ProVerif. We start with the formalization of the protocol into applied pi-calculus, which is used as input for ProVerif. After that, we will explain the necessary conditions that our protocol needs to fulfill in order to convey the required security properties. These conditions will be checked using ProVerif. However, although secrecy and authenticity are main requirements of our protocol, but we must also assure usability. In Section 5.5 we consider some usability aspects, along with the results of a usability test carried out with real users.

5.1 Formalization

Security protocols can be interpreted as concurrent systems, and thus they can be modelled using process calculi [13]. Pi-calculus is one of those calculi, and it has been successfully applied to model and analyse cryptographic primitives. Nevertheless, the application of pi-calculus to this matter is not straightforward. It had to be modified, and thus the spi-calculus and applied pi-calculus were proposed. In this work we use Proverif, which is a practical implementation of applied pi-calculus. Next, we describe how our protocol has been defined according to the notation of Proverif. Since the focus is on the application of the tool to our setup, the inner details of pi- and spi-calculus are not explained. The reader is referred to [29, 1] for further details.

We summarize the main components we used in Listing 1. In addition, in the formalization of the protocol the principals (*user, ws, ra, ca*) are noted using lower case letters to avoid confusion; when not referring to the formalization, principals are denoted with capital letters (User, WS, RA, CA). Different messages are exchanged in each of those processes, which are labelled according to the pattern *msgX*, with *X* ranging from 1 to 10, plus an extra message *msgcode* which is sent during the multichannel authentication. In the four processes (User, WS, RA and CA) *net* represents a public channel, which means that the attacker can eavesdrop on it, insert messages, and so on. The private channel *securemobilephonechannel* is the one used for multichannel authentication and the also private channels *privateSSLuserchannel* and

privateSSLwschannel are used for SSL negotiation.

```

out(c,m) : Sends the message m through the channel c
in(c,m) : Receives the message m through the channel c
new n : Creates the new name n
P|Q : Given the processes P and Q, executes both in parallel
!P : Given the process P replicates it any number of times

```

Listing 1: Basics of the pi-calculus notation.

As mentioned above, our registration protocol is built upon four different processes, simulating the principals of the protocol, plus two processes to simulate SSL negotiation between the User/attacker and the WS. We show below these processes, plus the preamble with the functions, types and queries definitions. Additionally, the complete source code is available at [16].

Preamble (Listing 2) The preamble is where the data types, functions, events, queries, etc. are defined in ProVerif. In our case, we use typical encryption/decryption functions, plus specialized functions for encryption/decryption of digital identities. We also define private channels for SSL negotiation and SMS sending, and several selfdescriptive data types and free variables.

```

1  (** Data types **)
2  type Host.
3  type Nonce.
4  type Key.
5  type Tag.
6  type Ticket.
7  type Id.
8  type Eid. (* Encrypted Id *)
9  type Link.
10
11  (** Channels **)
12
13  (* A public channel. *)
14  free net:channel.
15
16  (* A secure channel used for multichannel authentication *)
17  free securemobilephonechannel:channel [private].
18
19  (* A private channel for SSL negotiations. *)
20  free privateSSLuserchannel:channel [private].
21
22  (* A private channel for SSL negotiations. *)
23  free privateSSLwschannel:channel [private].
24
25
26  (** Principals **)
27  free ws,ra,ca:Host. (* The servers names. *)
28
29  (** Message tags. **)
30  free msg1,msg2,msg3,msg4,msg5,msg6,msg7,msg8,msg9,msg10:Tag
31  free msgcode:Tag.
32

```

```

33      (** Constructors and destructors **)
34
35      (* Encryption and decryption *)
36      fun encrypt(bitstring,Key):bitstring.
37      reduc forall m:bitstring, k:Key; decrypt(encrypt(m,k),k) = m.
38
39      (* ID encryption and decryption *)
40      (* We use different functions for ID encryption/decryption
41         for the secrecy queries *)
42      fun encryptid(Id,Key):Eid.
43      reduc forall id:Id, k:Key; decryptid(encryptid(id,k),k) = id.
44
45      (** Events **)
46      event UserRequestsRegistration(Host).
47      event WSSendsSMS(Host,Nonce).
48      event UserProcessesSMS(Host,Nonce).
49      event WSSendsLink(Host,Link).
50      event RASendsTicket(Host,Ticket).
51      event UserReceivesRegistrationData(Host,Ticket,Link).
52      event UserReceivesId(Host,Id).
53      event CASendsId(Host,Id).
54
55      (** The queries. **)
56
57      (* Secrecy *)
58
59      (* The ID must remain secret both the encrypted and
60         unencrypted versions*)
61      query id:Id, k:Key; attacker(encryptid(new id,k)).
62      query id:Id; attacker(new id).
63
64      (* Authenticity *)
65
66      (* Each time the CA generates and sends an ID to a
67         user h, it is because that user h has requested an
68         ID at least once *)
69      query h:Host, id:Id;
70      inj-event(CASendsId(h, id)) ==>
71          event(UserRequestsRegistration(h)).
72
73      (* Each time a user receives an ID, it has been
74         sent by the CA *)
75      query h:Host, id:Id;
76      inj-event(UserReceivesId(h,id)) ==>
77          inj-event(CASendsId(h,id)).
78
79      (* Each time a user processes an SMS, he has previously
80         requested it and it has been sent by the WS *)
81      query h:Host, c:Nonce;
82      inj-event(UserProcessesSMS(h,c)) ==>
83          (inj-event(WSSendsSMS(h,c)) &&
84           inj-event(UserRequestsRegistration(h))).
85
86      (* Each time a user receives the registration data (link and
87         ticket), the link has been sent by the WS and the ticket
88         by the RA *)
89      query h:Host, t:Ticket, l:Link;

```



```

90   inj-event( UserReceivesRegistrationData(h,t,l)) ==>
91     (inj-event( WSSendsLink(h,l)) &&
92       inj-event( RASendsTicket(h,t) )).
93
94   (* query h:Host , c:Nonce;
95     inj-event( WSSendsSMS(h,c)) ==>
96       inj-event( UserRequestsRegistration(h)). *)

```

Listing 2: ProVerif's preamble.

Process User (Listing 3) The user first “creates” his personal data. After proving his identity sending the code he receives by SMS, he obtains the registration ticket and activation link, and uses them to finalize the registration, receiving his digital identity. Note that three SSL key negotiations are performed. The first corresponds with the initial registration request, after which the user will receive an SMS. Subsequently, the user will respond with that code and receive the registration ticket and activation link. These messages that the user sends or receives correspond to the messages 1, 2, 3 and 8 of Fig. 5 and 10 and 18 of Fig. 6.

```

1  (** The user process. **)
2  let userprocess =
3
4    (* "Create" user data *)
5    new u:Host;
6
7    (* Launches the SSL key negotiation process for this
8      1st session *)
9    out(privateSSLUserchannel,(u,ws));
10   in(privateSSLUserchannel,(=u,ws,ksslws1:Key));
11
12   (* Tells WS to start the registration process *)
13   event UserRequestsRegistration(u);
14   out(net, encrypt((msg1,u,ws),ksslws1));
15
16   (* After requesting to start the registration process, u
17     receives a code via SMS *)
18   in(securemobilephonechannel,(=u,code:Nonce));
19   event UserProcessesSMS(u,code);
20
21   (* Send the code via the net channel to confirm identity *)
22   out(privateSSLUserchannel,(u,ws));
23   in(privateSSLUserchannel,(=u,ws,ksslws2:Key));
24   out(net, encrypt((msgcode,u,ws,code),ksslws2));
25
26   (* Receives the registration ticket and the activation link *)
27   in(net,(cmsg4:bitstring,link:Link));
28   let (=msg4,=ws,=u,ticket:Ticket,=link) =
29     decrypt(cmsg4,ksslws2) in
30   event UserReceivesRegistrationData(u,ticket,link);
31
32   (* Launches the SSL key negotiation process for
33     this 3rd session *)
34   out(privateSSLUserchannel,(u,ws));
35   in(privateSSLUserchannel,(=u,ws,ksslws3:Key));

```

```

36
37   (* Accesses the activation link and provides the registration
38      ticket *)
39   new k:Key;
40   out(net, (encrypt((msg5,u,ws,ticket,link,k),ksslws3), link))
41
42   (* Receives the digital identity *)
43   in(net, cmsg10:bitstring);
44   let (=msg10,=ws,=u,eid:Eid) = decrypt(cmsg10, ksslws3) in
45   let id = decryptid(eid,k) in
46   event UserReceivesId(u,id);
47   0.

```

Listing 3: Process User.

Process WS (Listing 4) The WS receives the initial registration request from a user (or the attacker). Sends an SMS via the *securemobilephonechannel* and after receiving back the code, it requests a registration ticket to the RA and generates an activation link. When the link is accessed, it makes a request for a digital identity and finally forwards it to the user. The same SSL negotiations are performed here than in the user process. Note also that, since the WS and the RA are trusted third parties not in control of the attacker, we deliver them a symmetric key for securely communicating between them from the beginning. The messages sent or received by the WS correspond with the messages in steps 1, 2, 3, 4, 6 and 8 of Fig. 5 and 10, 12, 17 and 18 of Fig. 6.

```

1  (** The ws process. **)
2  let wsprocess(kwsra:Key) =
3
4      (* Waits until someone starts the 1st SSL key negotiation *)
5      in(privateSSLwschannel, (u:Host,=ws,ksslws1:Key));
6
7      (* Receives the request to start the registration process *)
8      in(net, cmsg1:bitstring);
9      let (=msg1,=u,=ws) = decrypt(cmsg1, ksslws1) in
10
11      (* After establishing the SSL session with u, the ws, knows who
12         u is, and sends him a code via the extra secure channel
13         - that is, by SMS *)
14      new code:Nonce;
15      event WSSendsSMS(u,code);
16      out(securemobilephonechannel, (u, code));
17
18      (* Receives the keys of the 2nd SSL key negotiation *)
19      in(privateSSLuserchannel, (=u,=ws,ksslws2:Key));
20      in(net, cmsgcode:bitstring);
21      let (=msgcode, =u, =ws, =code) = decrypt(cmsgcode, ksslws2) in
22
23      (* Request a registration ticket to the RA, creates an
24         activation link and forward them to the user *)
25      out(net, encrypt((msg2,ws,ra,u),kwsra));
26      in(net, cmsg3:bitstring);
27      let (=msg3,=ra,=ws,=u,ticket:Ticket) = decrypt(cmsg3,kwsra) in

```

```

28  new link:Link;
29  event WSSendsLink(u,link);
30  out(net, (encrypt((msg4,ws,u,ticket,link),ksslws2), link));
31
32  (* Waits until the 3rd SSL key negotiation *)
33  in(privateSSLwschannel, (=u,ws,ksslws3:Key));
34
35  (* Processes the access to the activation link and forwards
36     the received registration ticket to the RA *)
37  in(net, (cmsg5:bitstring,=link));
38  let (=msg5,u,ws,ticket':Ticket,=link,k:Key) =
39                                     decrypt(cmsg5, ksslws3) in
40  out(net, encrypt((msg6,ws,ra,u,ticket',k),kwsra));
41
42  (* Receives the digital identity and forwards it to the user *)
43  in(net, cmsg9:bitstring);
44  let (=msg9,ra,ws,u,eid:Eid) = decrypt(cmsg9, kwsra) in
45  out(net, encrypt((msg10,ws,u,eid),ksslws3)).

```

Listing 4: Process WS.

Process RA (Listing 5) The RA receives a request from a user via the WS. After validating the user data, the RA creates a ticket for that user and sends it to the WS. When the ticket is received again, compares it to the one previously created. If they match, the RA makes a request to the CA for the generation of a digital identity for that user. In the end, the RA forwards the digital identity to the WS. The RA shares secret keys with the WS and the CA, pre-established from the beginning. The messages involving the RA correspond with messages 4 and 6 of Fig. 5 and 12, 14, 16 and 17 of Fig. 6.

```

1  (** The ra process. **)
2  let raprocess(kwsra:Key, kraca:Key) =
3
4      (* Receives the request for a new registration ticket *)
5      in(net, cmsg2:bitstring);
6      let (=msg2,ws,ra,u:Host) = decrypt(cmsg2, kwsra) in
7
8      (* Create the ticket and send it to the WS *)
9      new ticket:Ticket;
10     event RASendsTicket(u,ticket);
11     out(net, encrypt((msg3,ra,ws,u,ticket),kwsra));
12
13     (* Receive a supposedly legitimate registration ticket *)
14     in(net, cmsg6:bitstring);
15     let (=msg6,ws,ra,u,ticket':Ticket,k:Key) =
16                                     decrypt(cmsg6,kwsra) in
17
18     (* Checks the ticket. If everything is OK, request the CA
19        a new digital identity for the corresponding user *)
20     if ticket' = ticket then
21     out(net, encrypt((msg7,ra,ca,u,k),kraca));
22
23     (* Receive and forward the digital identity *)
24     in(net, cmsg8:bitstring);

```

```

25   let (=msg8,=ca,=ra,=u,eid:Eid) = decrypt(msg8, kraca) in
26   out(net, encrypt((msg9,ra,ws,u,eid),kwsra)).

```

Listing 5: Process RA.

Process CA (Listing 6) The CA only receives requests from the RA. For each request, the CA generates a digital identity with the user data received and sends the digital identity to the RA. The CA therefore shares a secret key with the RA, also pre-established from the beginning. These messages correspond with the messages 16 and 17 of Fig. 6.

```

1  (** The ca process **)
2  let caprocess(kraca:Key) =
3
4      (* Receives a request of a new digital identity *)
5      in(net,msg7:bitstring);
6      let (=msg7,=ra,=ca,u:Host,k:Key) = decrypt(msg7, kraca) in
7
8      (* Create the digital identity and send it to the RA *)
9      new id:Id;
10     let eid = encryptid(id,k) in
11     event CASendsId(u,id);
12     out(net, encrypt((msg8,ca,ra,u,eid),kraca)).

```

Listing 6: Process CA.

SSL negotiation processes (Listing 7) The user communicates with the WS through SSL channels. The corresponding keys are established using the process *sslkeynegotiationprocess*. We simulate the capability of the attacker to establish SSL sessions with the WS using the process *sslbypass*, which creates a key, makes it public, and sends it to the WS like a key created with a legitimate user.

```

1  (** SSL negotiation process **)
2  (* - used just between the User and WS *)
3  let sslkeynegotiationprocess =
4
5      (* u is the user who is supposedly establishing a SSL
6       session with WS a is who really is establishing the
7       SSL session WS *)
8      in(privateSSLUserchannel, (u:Host,=ws));
9
10     (* Creates the new SSL session key *)
11     new ksslws:Key;
12
13     (* Send the new SSL key through the privatesslchannel
14      channel, to let WS know the new key - and the user, in
15      case it is not the attacker who establishes the session *)
16     out(privateSSLUserchannel, (u,ws,ksslws));
17     out(privateSSLwschannel, (u,ws,ksslws)).
18
19  (** This process allows the attacker to establish SSL sessions
20   with the WS **)
21  let sslbypass =

```

```

22   in (net , (h:Host,=ws));
23   new ksslhws:Key;
24   out (net , ksslhws);
25   out (privateSSLwschannel , (h,ws,ksslhws)).

```

Listing 7: Processes for SSL negotiation.

Main process (Listing 8) The previous principals are called from the main process. In this process the secret shared keys between the trusted third parties are created. Obviously, we allow several replications for each principal.

```

1  (** The system. **)
2  process
3
4      (* Since the WS, RA and CA are trusted third parties , we can
5         establish symmetric keys for communications between them *)
6
7      new kwsra:Key;
8      new kraca:Key;
9
10     (* Launch all the processes *)
11     ( (!userprocess)                (* Users *)
12       | (!sslkeynegotiationprocess)  (* SSL negotiation *)
13       | (!sslbypass)                 (* Attacker SSL bypass *)
14       | (!wsprocess(kwsra))          (* Moodle Server *)
15       | (!raprocess(kwsra,kraca))    (* RA *)
16       | (!caprocess(kraca))         (* CA *)
17     )

```

Listing 8: Main process.

These four processes make up the fourth step in our methodology and, consequently, we can proceed with the security analysis of the registration protocol. In the next section we prove the security properties required in Section 4.1.

5.2 A quick introduction to ProVerif

ProVerif⁴ is an automatic formal verifier of security properties for communication protocols [10]. It accepts a formal definition of a protocol as pi-calculus instructions or Horn clauses [25], and a set of secrecy and/or events' correspondence queries to be proved. In both cases (pi-calculus and Horn clauses), the input is transformed into a set of Horn clauses which is completed and refined in a series of iterations. After the completion, a goal-directed depth-first search is carried out to prove the specified queries. Roughly speaking, secrecy verification is performed by applying ProVerif to assess if any of the implied terms can be derived from the obtained ruleset. To prove authenticity, we use ProVerif to test the possibility of creating an execution trace of the protocol in which any of the

⁴<http://www.proverif.ens.fr/>

events correspondences is broken. That is: if event A is supposed to happen before event B (because it is said so in a correspondence query) and ProVerif finds a trace in which that does not happen, then the correspondence is broken. Note that, by definition, an attacker is a process in which no event occurs [11].

To ask ProVerif to prove if a protocol keeps a given property, it has to be explicitly inquired about it using proper instructions. The output of ProVerif indicates if the queried security properties do or do not hold. If ProVerif finds that the property related to a specific query is false, it will show, along with an attack trace, something like⁵:

```
The attacker has the message property.
A trace has been found.
RESULT not attacker:property is false.
```

5.3 Secrecy

In ProVerif, secrecy properties can be checked with queries of the form:

```
query attacker(T).
```

Which is the way to ask ProVerif to test if the attacker can gain knowledge of some term T.

Since the aim of our protocol is to convey private digital identities to new users, these identities must remain secret. Moreover, in our protocol, the digital identities are sent encrypted under a symmetric key specified by the user. Therefore, even if this encrypted versions of the digital identities fall into the hands of an attacker, the secrecy is considered broken. More formally:

Definition 1. *CHAT-SRP preserves secrecy if neither the created digital identities nor their corresponding encrypted versions are disclosed to attackers.*

We check this in ProVerif with the queries in lines 61 and 62 of Listing 2. As a result, ProVerif informs that the corresponding secrecy properties are held. Therefore, given ProVerif’s soundness property, we have the guarantee that no attacker gains knowledge of the digital identities nor their encrypted versions.

5.4 Authenticity

The way of proving authenticity properties with ProVerif is by means of correspondence assertions [38, 12]. These correspondence assertions allow us to check, for instance, if a given event e always precedes another event e' . Since the attackers are, by definition, processes without events, if an event occurs, it must have been invoked by a *legitimate* process. Moreover, we can include

⁵We exclude some extra identifiers appended by ProVerif to the names, which are used to differentiate between different runs of the processes. Take into account that a single process can be executed several times, and ProVerif has to distinguish the different variables created in each run.

variables in these events, to see if a given variable has the same value in an event e than in another event e' .

Since, after a successful execution of our protocol, a new user acquires a digital identity which will be linked to him in the interactive platform, this identity must fulfill authenticity requirements (besides being kept secret). Specifically, we require that if the CA sends a digital identity to an user, then the legitimate corresponding user has requested it. This guarantees that no user receives a digital identity of a different user, and that only legitimate users can request a digital identity. We also need to guarantee that, every time a user receives a digital identity, it has been created by the CA. These requirements are more formally stated in definitions 2 and 3, respectively, corresponding to the lines 69 and 75 in Listing 2:

Definition 2. *If the CA issues a digital identity intended for a user h , then the legitimate user h must have requested it, at least once.*

Definition 3. *If a user receives a digital identity id , that digital identity id must have been issued by the Certification Authority.*

While the second requirement is held even if we do not make use of multichannel authentication, the first requirement does need this additional mechanism. To see this, one can delete lines 16 to 24 in Listing 3 and lines 11 to 21 in Listing 4 in order to eliminate the multichannel authentication in the formalization. After doing so, ProVerif finds a trace that contradicts the property required in definition 2. In short, after establishing an SSL session with the WS, the attacker provides all the required data in order to successfully impersonate some user. As a result, the attacker finally obtains an illegitimate, but valid, digital identity. This was the attack described in the first paragraph of section 4.3.

Therefore, this helps us see why we need to share some information with verified authenticity. The fact of using multichannel authentication enforces the robustness of our protocol. In any case, this multichannel exchange also needs to be verified. Namely, we will require that each time a user processes a code received via SMS, that same user has previously requested registration and the WS has send to him the same code. A logical consequence of this, captured in another requirement is that, each time a user receives a registration ticket and an activation link, then the RA has generated that same registration ticket and the WS has created the same activation link. These two requirements are formally stated in definitions 4 and 5, respectively, and are coded in lines 81 and 89 in Listing 2:

Definition 4. *Each time a user h processes an SMS with a code c , then the WS has send to that user h an SMS containing the code c , and the user h has also requested to be registered in the system.*

Definition 5. *Each time a user h receives a registration ticket t and an activation link l , then previously the RA has created the ticket t , the WS has created the link l , and both have sent them to the same user h .*

After running ProVerif with the previous correspondence assertions, it informs that the associated properties are kept. Again, ProVerif soundness guarantees the result.

Nonetheless, one more point is worth to be noted. In the multichannel alternative, the attacker is yet capable to start a registration process by providing the required data to the WS. But, in this case the WS will check if it knows the mobile phone number of the user who is allegedly requesting registration. If positive, the WS will send an SMS to the known number. When the real user receives the SMS, he will know that someone is trying to impersonate him, and he will ignore the SMS, and even inform the corresponding authority. Even though it was the attacker who started the registration, and not the real user, the WS will be sending an SMS to the correct number, and the registration will not succeed. This fact can be seen if we uncomment the query in line 95 of Listing 2, which informs us that a given user will not always process an SMS with a given code, even though the WS has previously sent it. This is not a weakness of the protocol. In fact, it is rather telling us that the multichannel authentication is working, because it serves to avoid impersonation.

5.5 Usability

As we have already said, usability and security inevitably lead to a tradeoff where the system designers must find an adequate equilibrium. In [23], the authors pinpoint some real situations where a system or protocol was not widely used, although a high level of security was implemented. All the reasons there stated concern usability: interface complexity, difficult configuration, etc. Moreover, they give examples of secure (but not usable) systems replaced by usable (but less secure) ones, even though the original purpose of both systems slightly differed.

It is even astonishing that, among the most known cryptographic principles, those written by Kerckhoffs in 1883 there is one principle referring this matter (see [27, page 12]). It is the last of 6 principles, and states:

Principle (Kerckhoffs). *Lastly, it is needed, given the circumstances that command its application, for the system to be easily usable, not requiring mental strain nor the knowledge of a long series of rules.*

The problem here is that there is no exact or even approximate equation, theory or whatever that could tell if a system is 100% usable. Therefore, the approach we have taken here is to base our work in concepts that are familiar to the vast majority of the potential users of our protocol (that will ease its understanding). Regarding the base and familiar concepts of our system, we can resume the protocol in three of them:

1. **EBIA**: Email Based Identification and Authentication ([22]). It is the starting point we took for our protocol. It links each user identity to his or her email account. As emails are something to which everyone is used nowadays, it keeps the property of familiarity.

2. **Tickets:** They are used to strengthen the basic EBIA system. Created from a chaotically-generated random number concatenated with some user dependent data. They serve to univocally link each specific user with a single registration request. They are used as a nonces, so once used, they are deleted in order to avoid multiple registrations. As we said in [17], everyone is used to get tickets in real life and keep them as a receipt to prove something later (e.g., to return clothes). Therefore, it also keeps the property of familiarity.
3. **SMS:** When used the multichannel authentication combining emails and SMS, the user will receive a short PIN into his mobile phone. Although this might not be a very common practice yet, it is gaining popularity, and mobile phones take a central roles in technology users nowadays. It seems then that, when used, this option still keeps the property of familiarity.

Keeping the familiarity, what remains is to create a friendly, self-descriptive, intuitive and as simple as possible interface, and that will not depend on the protocol itself. Nevertheless, the best, and maybe the only, way to foresee the users acceptance, is to test the system with real and potential users. Therefore, as a proof of concept, we performed some trials with real and potential users (students at our university). In these trials, the users were given a global description of the system. After the introduction, they had to register themselves in the Moodle test platform⁶. The registration process tested did not include the two-factor authentication scheme including SMS, but just the activation email and the ticket. At last, they were requested to fill up a questionnaire with the questions related to the adjectives in Table 1. From those tests we gained very valuable feedback and quite positive opinions, which are summarized in Table 1.

Adjective	Mean score (1 to 5)
Simple	3.60
Quick	4.20
Intuitive	3.19
Well developed	4.26
Secure	4.86
Useful	4.65
Trustworthy	4.73
Advisable for use	4.73

Table 1: Results of the trials performed with real users to measure the usability of the protocol. For each question, concerning an adjective describing the system, the user had to answer with a numerical score, ranging from 1 to 5, where 1 meant “Completely disagree” and 5 meant “Completely agree”. A total of 15 persons took the test.

⁶They also had to digitally sign an online exam, but we do not treat that matter here.

In the results, the first four adjectives can be considered as directly related to usability. The last four, although not directly related, will get bad scores may the user not understand or not know how to use the system, so they can also be seen as indirect measures of usability. Moreover, the users still have a sense of being using a secure system, which increases their confidence on the system, considering it trustworthy and advisable for use, may they find themselves in a situation in which they had to decide whether to incorporate the protocol or not. This latter property is quite important, because it highlights that the users admit a slight loss in usability (that is inevitable) in order to gain in security. Nevertheless, we have obtained very valuable feedback during the tests, regarding usability, and hope to be able to improve it.

6 Conclusion

In this work we have presented a new registration protocol for interactive and collaborative platforms, CHAT-SRP (**CHA**os based **T**ickets-**S**ecure **R**egistration **P**rotocol), which provides a very reasonable tradeoff between security and usability.

We have taken as starting point the EBIA model, which provides us a good reference from the usability perspective, since it is the most widely used protocol for registration in interactive platforms. As for its security, we have circumvented the two main problems inherent to these protocols. Namely, we prevent impersonation (with an authenticated extra channel) and MITM attacks (with the incorporation of registration tickets). Nevertheless, we still required to formally verify that our measures successfully avoid those weaknesses. Therefore, to evaluate the security of the protocol we have followed a methodology divided in interconnected phases. Obviously, the first one was to determine the protocol goals, which for us is to provide the new users with a digital identity. Once known that, we have established a general security model (the Dolev-Yao model, which assumes that the protocol uses perfect and unbreakable cryptographic primitives), in order to be available later to check if the required properties are held. After setting the general security model, we have defined the security requirements. In our case, we required secrecy and authenticity for the distributed digital identity. The next logical step is to formalize the protocol in a language suitable for being analyzed with formal tools, task undertaken in Section 4. We have used the applied pi-calculus for that purpose. At last, it remains to formally verify that the required properties are held. We have made use of ProVerif to verify them. In Section 5 we proved these properties along with a usability analysis of the protocol.

As we have proved using ProVerif (Section 5.3), our protocol keeps the secrecy of the digital identities, and it also keeps the authenticity property (Section 5.4) when facing both internal and external attackers. Of course, both according to the security model we have assumed. It does so by the combination of a multichannel authentication method (with some previous knowledge in the form of a mobile phone number) and of a registration ticket we have introduced to

univocally link each user with his corresponding request during the whole process. This ticket is created by introducing chaos based pseudo-random nonces, concatenated with the user email, which is used as preliminary identifier.

We have made use of concepts familiar to the users: EBIA, tickets, and SMS. Nevertheless, for measuring the usability there is no more precise science than usability tests involving real users. For that purpose, we have carried out some trials with potential users. For the tests, we incorporated our protocol (without the two-factor SMS authentication) into a Moodle platform, which is the perfect scenario for testing our protocol. As a result of the distribution of digital identities, the users who took part in the test were able to deliver digitally signed online exams, and became the first users to do so in our university. After the tests, they filled up a questionnaire asking about their experience with the system. The obtained results have been shown in Section 5.5. From them we can conclude that the acceptance is high, although we can still improve it. Besides, we received very valuable feedback.

As a result of providing digital identities to users of such collaborative and interactive systems, a full range of new cryptographically robust functionality is available for them. This provides greater security than using just SSL protected communications, since the users can now authenticate themselves with their digital identities. They could do it with SSL, may they have a digital identity, but they would not have one until our protocol (or other similar) provides them with one. Also, the fact of distributing digital identities in a standard format (like X.509), opens very interesting possibilities, like seamlessly adding advanced functionalities like privacy-friendly authentication and anonymity [28, 9]. Moreover, as we have seen from the tests, the users do perceive a greater security when they have their personal digital identity available (justified, as we have seen). This makes them have a greater trust in the system, increasing their acceptance, as they usually have to provide sensitive data to this kind of systems.

Acknowledgments

This work was supported by the UAM project of Teaching Innovation and the Spanish Government project TIN2010-19607. The work of David Arroyo was supported by a Juan de la Cierva fellowship from the Ministerio de Ciencia e Innovación of Spain.

References

- [1] Martín Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The spi calculus. In *ACM Conference on Computer and Communications Security*, pages 36–47, 1997.
- [2] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). In *IFIP TCS*, pages 3–22, 2000.

- [3] Gonzalo Álvarez and Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *I. J. Bifurcation and Chaos*, 16(8):2129–2151, 2006.
- [4] José Amigó. Chaos-based cryptography. In Ljupco Kocarev, Zbigniew Galias, and Shiguo Lian, editors, *Intelligent Computing Based on Chaos*, volume 184 of *Studies in Computational Intelligence*, pages 291–313. Springer Berlin / Heidelberg, 2009.
- [5] Ross J. Anderson. *Security engineering - a guide to building dependable distributed systems (2. ed.)*. Wiley, 2008.
- [6] Christian Haack Alan Jeffrey Andrew D. Gordon. Cryptyc: cryptographic protocol type checker. <http://cryptyc.cs.depaul.edu/>, 2002.
- [7] David Arroyo, Gonzalo Alvarez, José María Amigó, and Shujun Li. Cryptanalysis of a family of self-synchronizing chaotic stream ciphers. *Communications in Nonlinear Science and Numerical Simulation*, 16(2):805–813, 2011.
- [8] David Arroyo, Rhouma Rhouma, Gonzalo Alvarez, Shujun Li, and Veronica Fernandez. On the security of a new image encryption scheme based on chaotic map lattices. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 18:033112, 7 pages, 2008.
- [9] Vicente Benjumea, Seung Geol Choi, Javier Lopez, and Moti Yung. Anonymity 2.0 - x.509 extensions supporting privacy-friendly authentication. In *CANS*, pages 265–281, 2007.
- [10] Bruno Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *CSFW*, pages 82–96, 2001.
- [11] Bruno Blanchet. From secrecy to authenticity in security protocols. In *SAS*, pages 342–359, 2002.
- [12] Bruno Blanchet. *ProVerif Automatic Cryptographic Protocol Verifier User Manual*. CNRS, Département d’Informatique École Normale Supérieure, Paris, July 2010.
- [13] Xiaojuan Cai. A pure labeled transition semantics for the applied pi calculus. *Inf. Sci.*, 180(22):4436–4458, 2010.
- [14] Ellick Chan, Carl A. Gunter, Sonia Jahid, Evgeni Peryshkin, and Daniel Rebolledo. Using rhythmic nonces for puzzle-based dos resistance. In *CSAW*, pages 51–58, 2008.
- [15] Claudia Diaz. Anonymity and privacy in electronic services. phd, Katholieke Universiteit Leuven, Leuven, Belgium, December 2005.
- [16] Jesus Diaz, David Arroyo, and F.B. Rodriguez. Code of wep-ska for proverif. <http://www.ii.uam.es/~gnb/chat-srp.pv>, 2012.

- [17] Jesus Diaz, David Arroyo, and Francisco B. Rodriguez. An approach for adapting moodle into a secure infrastructure. In *CISIS*, pages 214–221, 2011.
- [18] Danny Dolev and Andrew Chi-Chih Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.
- [19] Mohamed Al Fairuz and Karen Renaud. Multi-channel, multi-level authentication for more secure ebanking. In *ISSA*, 2010.
- [20] Amparo Fúster-Sabater and Pino Caballero-Gil. Chaotic modelling of the generalized self-shrinking generator. *Appl. Soft Comput.*, 11(2):1876–1880, 2011.
- [21] Víctor Manuel Álvarez García, María del Puerto Paule Ruíz, and Juan Ramón Pérez Pérez. Voice interactive classroom, a service-oriented software architecture for speech-enabled learning. *J. Network and Computer Applications*, 33(5):603–610, 2010.
- [22] Simson L. Garfinkel. Email-based identification and authentication: An alternative to pki? *IEEE Security & Privacy*, 1(6):20–26, 2003.
- [23] Peter Gutmann and Ian Grigg. Security usability. *IEEE Security & Privacy*, 3(4):56–58, 2005.
- [24] Joshua D. Guttman, Jonathan C. Herzog, John D. Ramsdell, and Brian T. Sniffen. Programming cryptographic protocols. In *TGC*, pages 116–145, 2005.
- [25] Alfred Horn. On sentences which are true of direct unions of algebras. *J. Symb. Log.*, 16(1):14–21, 1951.
- [26] Christos Kalloniatis, Petros Belsis, and Stefanos Gritzalis. A soft computing approach for privacy requirements engineering: The pris framework. *Appl. Soft Comput.*, 11(7):4341–4348, 2011.
- [27] Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5–83, January 1883.
- [28] Taekyoung Kwon. Privacy preservation with x.509 standard certificates. *Inf. Sci.*, 181(13):2906–2921, 2011.
- [29] Robin Milner, Joachim Parrow, and David Walker. A calculus of mobile processes, i. *Inf. Comput.*, 100(1):1–40, 1992.
- [30] Shintaro Mizuno, Kohji Yamada, and Kenji Takahashi. Authentication using multiple communication channels. In *Digital Identity Management*, pages 54–62, 2005.

- [31] C. Neuman, T. Yu, S. Hartman, and K. Raeburn. The kerberos network authentication service (v5). RFC 4120 (Proposed Standard), July 2005. Updated by RFCs 4537, 5021, 5896, 6111, 6112, 6113.
- [32] Cleber K. Olivo, Altair O. Santin, and Luiz S. Oliveira. Obtaining the threat model for e-mail phishing. *Applied Soft Computing*, (0):–, 2011.
- [33] A. B. Orue, Gonzalo Álvarez, A. Guerra, G. Pastor, M. Romera, and F. Montoya. Trident, a new pseudo random number generator based on coupled chaotic maps. In A. Herrero and et al., editors, *3rd Int. Workshop on Computational Intelligence in Security for Information Systems (CISIS'10)*, *AISC 85*, pages 183–190, León (Spain), 2010. Springer-Verlag.
- [34] P. Ryan and S. Schneider. *The modelling and analysis of security protocols: the CSP approach*. Addison-Wesley Professional, first edition, 2000.
- [35] Edgar Weippl and Martin Ebner. Security & privacy challenges in e-learning 2.0. 2008.
- [36] Komminist Weldemariam, Richard A. Kemmerer, and Adolfo Villafiorita. Formal analysis of an electronic voting system: An experience report. *Journal of Systems and Software*, 84(10):1618–1637, 2011.
- [37] Ford-Long Wong and Frank Stajano. Multi-channel protocols. In *Security Protocols Workshop*, pages 112–127, 2005.
- [38] T.Y.C. Woo and S.S. Lam. A semantic model for authentication protocols. In *Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer Society Symposium on*, pages 178 –194, may 1993.